**U.S. Department of Transportation**

Office of the Secretary of Transportation

400 Seventh St., S.W.
Washington, D.C. 20590

May 7, 1999

MEMORANDUM TO: Financial Management Committee Members

FROM: A. Thomas Park A Thomas Park
Director of Financial Management

ACTION: DAFIS Feeder System Survey

The purpose of the attached memorandum of understanding is to provide a security assurance agreement (memorandum of understanding) between the sponsor of the Departmental Accounting and Financial Information System (DAFIS), Office of Financial Management, Office of the Secretary, Department of Transportation and sponsors of each of the DAFIS feeder systems. National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems requires memorandums of understanding between systems sharing sensitive information.

The completion of system security plans is a requirement of the Office of Management and Budget (OMB-130), "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," updated in 1996, and of Public Law 100-235, "Computer Security Act of 1987."

In order for a security plan to adequately reflect the protection of ADP resources, a management official must authorize a system to process information to operate. The Authorization of a system to process information, granted by a management official, provides an important quality control (Note: Some agencies refer to this authorization as accreditation). DAFIS was accredited in September of 1997 and provides a secure environment for data received from feeder systems.

Attached is a Memorandum of Understanding (Attachment A) that outlines the responsibilities of sponsors of systems sharing information with DAFIS. Attachment B provides you with a DAFIS and DAFIS Feeder Systems Data Sensitivity Rating. Attachment C, the DAFIS Feeder System Assurance Statement, should be completed for any uncertified DAFIS feeder system. Attachment D contains the most recent list of DAFIS feeder systems that we have for your organization. Attachment A and C requires feeder systems sponsor's signature.

Please provide to my office no later than 6/30/99 the signed Memorandum of Understanding with the information requested for each of your systems that is presently feeding information into DAFIS. If you have any questions please contact Eric Brown, (202) 366-5651.

Attachments

# MEMORANDUM OF UNDERSTANDING (MOU)

During December 1998, NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems was published which interpreted OMB-130 and defined requirements for accreditation. The NIST 800-18 categorizes each system as either a "major application" or as a "general support system." An example of a major application is an accounting system whereas an example of a general support system is a LAN or the telecommunications network that supports the accounting system.

The 800-18 requires the DAFIS sponsor to maintain the following information from connecting systems or systems sharing information with DAFIS. Therefore, we are requesting that your organization provide to this Office no later than 6/30/99 the following information for each DAFIS feeder system(s) for which you are responsible.

- Name of system(s);____________________________________________
- Organization owning system(s);________________________________
- Type of interconnection (TCP/IP,Dial-up,SNA,Manual);__________
- Name and title of security certification accrediting management official(s);______________________________________
- Date of accreditation (If not certified, please complete Attachment B);______________________
- Sensitivity level of system._________

DAFIS is a Level CS2 based upon the data sensitivity rating as described in Attachment B.

____________________________________________ __________
(Signature/Title of Feeder System Sponsor) Date

Attachment A

## DAFIS AND DAFIS FEEDER SYSTEM DATA SENSITIVITY RATING

(DAFIS and DAFIS feeder systems have a CS2 data sensitivity rating as described below)

### Information Categories

| Category | | Explanation and Examples |
|---|---|---|
| Number | Name | |
| 1 | Information about persons | Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history). |
| 2 | Financial, budgetary, commercial, proprietary and trade secret information | Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures. |
| 3 | internal administration | Information related to the internal administration of DOT. Includes personnel rules, bargaining positions, and advance information concerning procurement actions. |
| 4 | Investigation, intelligence-related, and security information (14 CFR PART 191.5(D)) | Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements. |
| 5 | Other Federal agency information | Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency. |
| 6 | New technology or controlled scientific information | Information related to new technology; scientific information that is prohibited from disclosure to certain foreign governments or that may require an export license from the Department of State and/or the Department of Commerce. |
| 7 | Mission-critical information | Information designated as critical to an FAA mission, includes vital statistics information for emergency operations. |
| 8 | Operational information | Information that requires protection during operations; usually time-critical information. |
| 9 | Life-critical information | Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life). |
| 10 | Other sensitive information | Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare. |
| 11 | System configuration management information | Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at FAA; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information. |
| 12 | Public information | Any information that is declared for public consumption by official DOT authorities. This includes information contained in press releases approved by the Office of Public Affairs, Office of Civil Aviation Security or other official DOT source. It also includes Information placed on public access world-wide-web (WWW) servers. |

Attachment B

## Security Levels for Information Systems

| CS Security Level | Impact Description | Explanation |
|---|---|---|
| CS1 | Moderately serious | • Noticeable impact on DOT missions, functions, image, or reputation. A breach of this security level would result in a negative outcome; or<br>• Would result in DAMAGE, requiring repairs, to an asset or resource. |
| CS2 | Very serious | • Severe impairment to DOT's missions, functions, image, and reputation. The impact would place DOT at a significant disadvantage; or<br>• Would result in MAJOR damage, requiring extensive repairs to assets or resources. |
| CS3 | Catastrophic | • Complete loss of mission capability for an extended period; or<br>• Would result in the loss of MAJOR assets or resources and could pose a threat to human life. |

## Relationship Between Information Categories and *Minimum* Security Levels for IS

| Information Category | | *Minimum* CS Security Level | | |
|---|---|---|---|---|
| # | | CS1 | CS2 | CS3 |
| 1 | Information about persons | | X | |
| 2 | Financial, budgetary, commercial, and trade secret information | | X | |
| 3 | DOT internal administration | | X | |
| 4 | Investigation, intelligence-related, and security information | | | X |
| 5 | Other Federal agency information | | X | |
| 6 | New technology or controlled scientific information | | X | |
| 7 | Mission-critical information | | | X |
| 8 | Operational information | | X | |
| 9 | Life-critical information | | | X |
| 10 | Other information | X* | | |
| 11 | System configuration management information | | X | |
| 12 | Public information | X* | | |

## DEPARTMENTAL
## ACCOUNTING AND FINANCIAL INFORMATION SYSTEM
## (DAFIS)

### FEEDER SYSTEM ASSURANCE STATEMENT

Name of agency or
Operating Administration: ______________________________

Point of Contact: ______________________________________

Telephone Number: ______________________________________

Based on a review of the feeder system security plan, requirements set forth in OMB Circular A-130, and the security requirements of (Name of DAFIS Feeder System): ______________________________________, the application was accredited on (Date) ____________.

If the feeder system has not been accredited, please specify the expected accreditation date ____________.

Please check here [ ] if the feeder system has never been accredited.

Please indicate below the reasons for deferring accreditation.

[ ] The feeder system will be terminated within the next year and the replacement system will be accredited before it is implemented.

[ ] No Security Plan.

[ ] An analysis of threats, vulnerabilities, and safeguards has not been performed within the last three years.

[ ] No documented security specifications exist.

[ ] Documented testing of security specifications has not been performed within the last three years.

[ ] Major vulnerabilities exist (specify)__________

[ ] Security awareness training has not been performed.

[ ] No disaster recovery/contingency plan.

[ ] Other ______________________________

________________________________________________
(Signature/Title of Accrediting Program Official)

Attachment C

# Security Status of DAFIS Feeder Systems

TASC

USCG

FAA

FHWA

FRA

NHTSA

FTA

MARAD

VOLPE

Attachment D